AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Maine

U.S. DISTRICT COURT
BANGOR, MAINE
RECEIVED AND FILED
2016 NOV 17 P 3:51
DEPUTY CLERK

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH FACEBOOK USER ID "100005109483224" THAT IS STORED AT PREMISES CONTROLLED BY FACEBOOK, INC.

Case No. 1:16-mj-00240-JCN

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

INFORMATION ASSOCIATED WITH FACEBOOK USER ID "100005109483224" THAT IS STORED AT PREMISES CONTROLLED BY FACEBOOK, INC., MORE FULLY DESCRIBED IN ATTACHMENT A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2252A(a)(5)(B) and 2252A(a)(2) and 2252(a)(2)	Possession of child pornography and distribution and receipt of child pornography

The application is based on these facts:
Affidavit of Gregory M. Kelly, Special Agent, Homeland Security Investigations

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Gregory M. Kelly, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/17/16

Judge's signature

City and state: Bangor, Maine

John C. Nivison, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Facebook User ID **100005109483224** that is stored at premises owned, maintained, controlled, or operated by Facebook, Inc. a company headquartered in Menlo Park, California.

Account associated with Preservation Request 905851

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 14, 2016, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

b. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

c. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

d. All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings;

rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

e. All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

f. All "check ins" and other location information;

g. All IP logs, including all records of the IP addresses that logged into the account;

h. All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

i. All information about the Facebook pages that the account is or was a "fan" of;

j. All past and present lists of friends created by the account;

k. All records of Facebook searches performed by the account;

l. All information about the user's access and use of Facebook Marketplace;

m. The types of service utilized by the user;

n. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

o. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

p. All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

The Provider shall disclose responsive data, if any, by sending to Homeland Security Investigations, 324 Harlow Street, Bangor, Maine 04401 using the US Postal Service or another courier service, notwithstanding 18 U.S.C. 2252A or similar statute or code.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of **18 U.S.C. 2252A(a)(2) and (a)(5)(B)** as well as **18 U.S.C. 2252(a)(2) and 2252A(a)(2)**, those violations involving the user(s) of the account and occurring on or after March 17, 2016, including, for each user ID identified in Attachment A, information pertaining to the following matters:

a. Violations of Title 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B) (possession of child pornography);

b. Violations of Title 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2) (distributing and receiving child pornography);

c. Records or information pertaining to an interest in child pornography;

d. Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;

e. Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;

f. Records relating to the identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

g. Records relating to the identity of the person(s) who communicated with the user ID concerning the identity and location of the account user, an interest in child pornography, or the trading in child pornography, including records that help reveal the whereabouts or any such person(s).

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FACEBOOK USER ID "**100005109483224**" THAT IS STORED AT PREMISES CONTROLLED BY FACEBOOK, INC.	Case No. 1:16-mj-00240-JCN **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Gregory M. Kelly, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user account that is stored at premises owned, maintained, controlled, or operated by Facebook, Inc., ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate items described in Section II of Attachment B.

2. I am a Special Agent (SA) with Homeland Security Investigations (HSI), and have been since 2007. Since approximately May 2010, I have been assigned to conduct investigations of crimes where computers and the Internet are used in the sexual exploitation of children, including (but not limited to) violations of 18 U.S.C. Sections 2252 and 2252A, which

prohibit a person from knowingly transporting, receiving, distributing, possessing or accessing with intent to view, in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, child pornography, as defined in 18 U.S.C. Section 2256(8). I have received formal and on-the-job training in the investigation of cases involving the sexual exploitation of children. My experience includes participation in the execution of numerous search warrants involving child pornography and seizures of computers and other storage media, and I have participated in numerous arrests and interviews of subjects involved with child pornography and child exploitation.

3. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

4. The facts set forth in this affidavit are based on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2252A(a)(5)(B), possession of child pornography, and 2252A(a)(2) and 2252(a)(2) distribution and receipt of child pornography have been committed by Derrick Coffin. There is also probable cause to search the information described in Attachment A for evidence related to these crimes, as described in Attachment B.

PROBABLE CAUSE

6. On March 18, 2016, personnel from the Lincoln, Maine Police Department and the State of Maine Probation Office conducted a probation check of Derrick Aaron Coffin at his residence located at 348 South Road in Lincoln, Maine. Coffin was on probation for a 2006 State of Maine conviction of Gross Sexual Assault for breaking into a home and forcing a 10-year-old boy to perform oral sex on him. The investigators conducted the probation check after receiving information that Coffin possessed child pornography on a thumb drive. As part of the probation check, the investigators detained a laptop computer, a cell phone, and an SD card for forensic review. A forensic review of the laptop computer revealed over 500 images of child pornography in allocated space and over 700 images of child pornography in unallocated space. The Lincoln Police Department contacted me for assistance with the investigation into the possession of child pornography.

7. On March 29, 2016, Bangor Police Department Sergeant Brent Beaulieu and I interviewed Coffin about the child pornography recovered from the laptop computer. Coffin denied searching for, downloading or possessing child pornography and theorized that someone must be breaking into his home while he was not there and searching for and viewing the child pornography in order to set him up. Coffin added that he was not normally home during the day and that he normally traveled to Bangor, Maine to look for work. Coffin stated that he used a program called Eraser to hide evidence of his illegal download of commercial movies, but denied using Eraser to hide evidence of his searching for and downloading child pornography. At the conclusion of the interview, Sergeant Beaulieu advised Coffin that his probation officer had placed a hold on him for the probation violation and subsequently arrested Coffin. Coffin has been incarcerated since this arrest on March 29, 2016.

8. I reviewed the forensic examination results of the laptop computer and noted that all the recovered child pornography files showed a last written date of March 17, 2016 between 3:31PM and 5:18PM. I focused my review of the forensics on March 17, 2016 and noted that someone had searched the Internet for files related to the sexual exploitation of children on March 17, 2016 between 1:58PM and 2:05PM. In addition, someone accessed pornography websites using the laptop from 2:14PM through 5:18PM. The type of pornography websites visited includes image sharing websites, webcam based websites, dating websites, general adult pornography websites and an underage model website. After reviewing the recovered child pornography files and the web browsing history, I was able to determine that many of the recovered child pornography files were downloaded from the Internet during the above noted period.

9. Through the course of this investigation, I learned that Coffin was also the subject of a probation check in May of 2015. At that time, his cell phone was forensically reviewed and his Internet search terms and web history were captured. I reviewed the forensic examination results from May 2015, compared them to the forensic examination results from the laptop computer seized in March 2016, and noted that similar search terms were recovered from both. For example, on May 4, 2015, someone using Coffin's cell phone entered the search terms, 'super sexy girls', 'super sexy young girls', and 'preteen sexy young girls' into YouTube. On March 2, 2016, someone using Coffin's laptop computer entered the search term, 'really sexy little kids' into YouTube. On May 27, 2015, someone using Coffin's cell phone entered the search term, 'young cheerleaders' into Google. On March 2, 2016, someone using Coffin's laptop computer entered the search terms, 'cheerleading' and 'child cheerleading' into YouTube. On May 27, 2015, someone using Coffin's cell phone entered the search term, 'young models'

into Google. On March 17, 2016, someone using Coffin's laptop computer entered the search terms, 'little young nn models', 'lolita young models', and 'underage model pics' into Google. I believe the fact that similar search terms were found on two separate devices used by Coffin indicate that it was likely Coffin himself who entered the search terms.

10. The forensic review of the laptop computer also revealed the presence of an anti-forensics program called Eraser. Eraser is a secure data removal tool for Windows that completely removes sensitive data from a hard drive by overwriting it several times with carefully selected patterns. I believe that the Eraser program was used by Coffin in an attempt to hide his online activities related to child pornography and is likely the reason the only child pornography files recovered from the allocated space of the laptop were last written less than 24 hours before an unannounced probation check was conducted. I believe that the probation check occurred before Coffin had an opportunity to remove the evidence of his online activities from March 17, 2016.

11. The forensic review of the laptop computer and cell phone seized as part of the probation check also revealed two Google accounts associated with Coffin which were identified as derrickacoffin82@gmail.com and derrickcoffin68@gmail.com as well as a Facebook account associated with the username derrickcoffin68@gmail.com.

12. I obtained basic Google account subscriber information and Internet Protocol (IP) login history for the derrickacoffin82@gmail.com and derrickcoffin68@gmail.com accounts. The name listed for the derrickacoffin82@gmail.com account was 'derrick aaron' and a recovery email address of derrickcoffin68@gmail.com was listed. The name listed for the derrickcoffin68@gmail.com account was 'Derrick Coffin' and no recovery email address was listed. The number of the cell phone seized from Coffin during the probation check was listed in

the subscriber information for both accounts indicating that Coffin was likely the user of the accounts. The IP login history revealed numerous Google account logins contemporaneous to the dates and times the child pornography was searched for and/or viewed. I obtained subscriber information for the IP address used to login to the Google accounts at these times and learned that the IP address had been assigned to Derrick Coffin at 348 South Road in Lincoln, Maine (hereafter referred to as 'Coffin's home IP address'). Coffin's home IP address was used to login to Coffin's Google accounts during the time the child pornography was searched for and/or viewed indicating that whoever accessed the Google accounts had to be using Coffin's home network. Multiple users were not logged into the account at the same time from different locations.

13. I also obtained basic Facebook account subscriber information and IP login history for the Facebook account associated with derrickcoffin68@gmail.com. Facebook provided the associated Facebook user ID as **100005109483224.** The subscriber information showed the name associated with the account as 'Joe Diffy' and the email address as derrickcoffin68@gmail.com. I have learned through the course of this investigation that Coffin had identified the 'Joe Diffy' Facebook account as his account to an ex-girlfriend. The phone number associated with the account was listed as 12072901571 which I have previously identified as Coffin's cell phone number. I also reviewed the IP login history for the Coffin Facebook account and noted a login to the account on March 17, 2016 at 1:31PM using Coffin's home IP address.

14. In addition to the Facebook account information, I reviewed the forensic examination results of Coffin's cell phone that had been searched as part of his probation check. I noted seven screen captures of Facebook profile pages belonging to women saved to Coffin's

cell phone that were created on March 17, 2016 between 1:12PM and 1:20PM. The filenames of these screen captures were consistent with filenames normally generated when a screen capture is created. For example, one of the screen captures was entitled, "2016-03-17-13-12-42". I know through my experience that this filename was likely not user created and was likely auto-generated by the operating system of the phone with the date and time that the file was created. I also noted that in these screen captures the time could be seen in the upper corner and that six of the seven screen captures time displayed corresponded with its file name. The seventh screen capture, entitled, "2016-03-17-13-20-00", did not display the time, but instead displayed the current Wi-Fi connection for the device which read, "Connected to 'Fairpoint5A39' (secure)". I recognized Fairpoint5A39 to likely be Coffin's home wireless network due to the fact that the forensic examination of Coffin's laptop computer showed Fairpoint5A39 as the only network profile associated with the laptop. The network profile creation date was noted as May 2, 2015 and the laptop showed a last connected date to the network of March 18, 2016. I know through this investigation that Coffin used Fairpoint Communications for his home internet service.

15. I also know from reviewing email messages recovered from Coffin's cell phone seized as part of the probation check that Coffin corresponded with numerous women via online accounts in order to coordinate sexual encounters. I believe Coffin likely screen captured the above-noted women's Facebook accounts in order to contact them and eventually attempt to coordinate a sexual encounter.

16. Based on the above, I believe Coffin was at home on March 17, 2016 and logged into his Google accounts and his Facebook account from his home wireless network while searching for and/or viewing child pornography. As previously noted, someone using Coffin's laptop computer searched the Internet for files related to the sexual exploitation of children on

March 17, 2016 between 1:58PM and 2:05PM. At the same time as the searches were being conducted, someone logged into Coffin's Google accounts using Coffin's home IP address. Approximately 27 minutes before someone searched the Internet for files related to the sexual exploitation of children using Coffin's laptop computer, someone logged into Coffin's Facebook account using Coffin's home IP address. From approximately 2:14PM through 5:18PM, after searching for files related to the sexual exploitation of children, someone accessed pornography websites via the Internet and viewed child pornography. I believe that person to be Coffin and I believe that Coffin's Facebook account will provide evidence of Coffin's presence at his home during the above noted activity.

17. I have probable cause to believe and I do believe that the content of the Facebook account associated with derrickcoffin68@gmail.com and the records associated with that account will provide evidence of the identity of the person accessing the account from Coffin's home IP address on March 17, 2016. I believe that Coffin likely corresponded with at least one of the seven women whose profiles he saved to his phone and that Facebook records will document this correspondence. I believe it possible that Coffin could have communicated with these women by Facebook instant messenger, by commenting on their photos, by "liking" their photos, by posting his own photo(s), or by other functions in Facebook and that these records will provide evidence that Coffin was home and accessing his Facebook account while the searching for and viewing of child pornography occurred on his laptop computer.

18. In addition, I believe Coffin could have corresponded with others on Facebook who could have been child pornography trading partners, those with an interest in child pornography, or other witnesses who could give insight into Coffin's whereabouts during the search for and download of child pornography. Due to Coffin's use of this account during the

time I believe he was searching for and accessing child pornography, it may contain evidence regarding crimes relating to the receipt, transportation, possession, or access with intent to view child pornography.

19. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

20. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

21. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

22. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

23. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

24. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a

user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

25. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

26. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

27. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

28. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

29. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through

the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

30. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

31. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

32. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

33. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

34. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings;

rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

35. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

36. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

37. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user

attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

38. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

39. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

40. Based on the forgoing, I request that the Court issue the proposed search warrant.

41. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

42. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Because the provider may retrieve this information at a time outside of normal Eastern Standard day-time hours, I believe there is reasonable cause to authorize the execution of this warrant at any time of the day or night.

REQUEST FOR SEALING

43. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These

documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Gregory M. Kelly
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on November 17, 2016

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Facebook User ID **100005109483224** that is stored at premises owned, maintained, controlled, or operated by Facebook, Inc. a company headquartered in Menlo Park, California.

Account associated with Preservation Request 905851

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 14, 2016, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

b. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

c. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

d. All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings;

rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

e. All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

f. All "check ins" and other location information;

g. All IP logs, including all records of the IP addresses that logged into the account;

h. All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

i. All information about the Facebook pages that the account is or was a "fan" of;

j. All past and present lists of friends created by the account;

k. All records of Facebook searches performed by the account;

l. All information about the user's access and use of Facebook Marketplace;

m. The types of service utilized by the user;

n. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

o. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

p. All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

The Provider shall disclose responsive data, if any, by sending to Homeland Security Investigations, 324 Harlow Street, Bangor, Maine 04401 using the US Postal Service or another courier service, notwithstanding 18 U.S.C. 2252A or similar statute or code.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of **18 U.S.C. 2252A(a)(2) and (a)(5)(B)** as well as **18 U.S.C. 2252(a)(2) and 2252A(a)(2)**, those violations involving the user(s) of the account and occurring on or after March 17, 2016, including, for each user ID identified in Attachment A, information pertaining to the following matters:

a. Violations of Title 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B) (possession of child pornography);

b. Violations of Title 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2) (distributing and receiving child pornography);

c. Records or information pertaining to an interest in child pornography;

d. Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;

e. Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;

f. Records relating to the identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

g. Records relating to the identity of the person(s) who communicated with the user ID concerning the identity and location of the account user, an interest in child pornography, or the trading in child pornography, including records that help reveal the whereabouts or any such person(s).

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Facebook and my official title is _____. I am a custodian of records for Facebook. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Facebook, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Facebook; and

c. such records were made by Facebook as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature